DERANGEMENTS IN FINITE CLASSICAL GROUPS FOR ACTIONS RELATED TO EXTENSION FIELD AND IMPRIMITIVE SUBGROUPS AND THE SOLUTION OF THE BOSTON–SHALEV CONJECTURE

JASON FULMAN AND ROBERT GURALNICK

Abstract. This is the fourth paper in a series. We prove a conjecture made independently by Boston et al and Shalev. The conjecture asserts that there is an absolute positive constant δ such that if G is a finite simple group acting transitively on a set of size $n > 1$, then the proportion of derangements in G is greater than δ. We show that with possibly finitely many exceptions, one can take $\delta = .016$. Indeed, we prove much stronger results showing that for many actions, the proportion of derangements goes to 1 as n increases and prove similar results for families of permutation representations.

1. Introduction

A permutation on a set X is called a derangement if it has no fixed points. A classical and elementary theorem of Jordan asserts that a finite group acting transitively on a set X of size at least 2 contains derangements. There are many results on the proportion of derangements in finite transitive groups. Rather amazingly, it was only recently that it was shown [CC] that if G acts transitively on a set of size $n > 1$, then the proportion of derangements is at least $1/n$ (this is a quite easy theorem – see [DFG] for a short proof and also an upper bound in terms of the rank of the permutation group).

Derangements come up naturally in many contexts (see the surveys [DFG] and [Se] for applications to topology, number theory, and maps between varieties over finite fields). Perhaps the earliest results on derangements are due to Montmort [Mo]. He studied derangements in the full symmetric group S_n to analyze a card game (it is easy to see that the proportion of derangements in S_n tends to $1/e$ as $n \to \infty$ and is always at least $1/3$).

If G is a finite simple group acting faithfully and transitively on a set X, then it was noticed that the proportion of derangements never seemed to be too small. This led Boston et al [BDF] and Shalev to (independently)

Date: Version of July 31, 2015.

Keywords: derangement, finite classical group, random matrix, permutation group.

2010 AMS Subject Classification: 20G40, 20B15.

Fulman was partially supported by NSA grant H98230-13-1-0219. Guralnick was partially supported by NSF grant DMS-1302886.

conjecture that there is a constant $\delta > 0$ so that for a finite simple group G, the proportion of derangements is at least δ. (Boston et al [BDF] suggest that $\delta = 2/7$; in fact that is not true – Tim Burness has observed that the group ${}^2F_4(2)'$ has a transitive permutation representation with the proportion of derangements equal to 89/325. We also mention that by [NP] that for d sufficiently large, the proportion of derangements for $SL(d,2)$ acting on 1-dimensional spaces is less than .29). In this paper, we complete the proof of the Boston-Shalev conjecture:

Theorem 1.1. *Let G be a finite simple group acting faithfully and transitively on a set X of cardinality n. With possibly finitely many exceptions, the proportion of derangements in G is at least .016.*

The result fails for general transitive groups (indeed, there are easy examples where the proportion of derangements is exactly $1/n$). It also fails for almost simple groups (it follows from our result that one can show the proportion of derangements for an almost simple group is at least $\delta/\log n$). Theorem 1.1 was proved for alternating and symmetric groups by Luczak and Pyber [LP]. Indeed, they proved some stronger results. Since the result is asymptotic, we can ignore sporadic groups and so we consider finite simple groups of Lie type (as in [LP], we prove stronger results).

This is the fourth paper in a series beginning with [FG4], [FG2], [FG1] and completes the proof. Indeed, we prove the following (recall an element of a finite group of Lie type is regular semisimple if its centralizer in the corresponding algebraic group has connected component a (maximal) torus).

Theorem 1.2. *There exists a $\delta > 0$ so that if G is a sufficiently large finite simple group of Lie type acting faithfully and transitively on a set X, then the proportion of elements which are both regular semisimple and derangements is at least δ.*

Note that it is not always the case that there exist derangements which are semisimple. The simplest example is to take $G = PSL(2,5) \cong A_5$ acting on 5 points. The only derangements are elements of order 5 which are unipotent. On the other hand by [GM], aside from a very small number of simple finite groups of Lie type, there exist semisimple regular conjugacy classes C_1 and C_2 such that no proper subgroup intersects both C_i (whence in any action either C_1 or C_2 consists of derangements); i.e. the group is invariably generated by C_1 and C_2 – that is if $x_i \in C_i$, then $G = \langle x_1, x_2 \rangle$.

Again, with possibly finitely many exceptions, one can take $\delta = .016$. In [FG4], the result was proved for finite groups of Lie type of bounded rank (and so in particular for the exceptional groups). Another proof was given in [FG2]. Thus, it suffices to consider the finite classical groups (e.g., linear, unitary, orthogonal and symplectic groups). In [FG2], it was shown that aside from the families (with regard to the natural module for the classical group):

(1) reducible subgroups;

(2) imprimitive subgroups (i.e. those stabilizing an additive decomposition of the spaces); and
(3) extension field subgroups (i.e. those stabilizing an extension field structure on the natural module).

that the proportion of derangements goes to 1 as the rank goes to ∞. Combining this result with [FNP] gives Theorem 1.2 for these actions.

In [FG1], reducible subgroups were considered and Theorems 1.1 and 1.2 were proved in that case. Moreover, it was shown that for the action on an orbit of either totally singular or nondegenerate subspaces (of dimension at most 1/2 the ambient space), the proportion of derangements goes to 1 if the dimension of the subspaces tended to ∞.

In this paper, we deal with the last two families. We will prove:

Theorem 1.3. *There exist universal positive constants A and δ satisfying the following. Let G be a finite classical group with natural module V of dimension n, and $V = V_1 \oplus \ldots \oplus V_b$. Let H be the stabilizer of this decomposition and assume that H is irreducible on V. Then the proportion of elements of G contained in a conjugate of H (for some b) is at most A/n^δ.*

We also prove the following result for GL.

Theorem 1.4. *There exist positive constants A and δ satisfying the following. Let $G = GL(n,q)$. Let $X(G)$ denote the union of all irreducible subgroups of G not containing $SL(n,q)$. Then the proportion of elements in any given coset of $SL(n,q)$ contained in $X(G)$ is at most A/n^δ.*

In the previous result, q can increase or be fixed. This result was proved by Shalev [Sh] for $GL(n,q)$ with q fixed using deep work of Schmutz [Sc] on orders of elements in general linear groups. Our technique is more elementary. In fact, one cannot do much better than the previous result. Suppose that $n = 2m$. The proportion of elements contained in $GL(m,q) \times GL(m,q) < GL(m,q) \wr S_2$ for q large is approximately the same as the proportion of elements in S_n which fix a subset of size m. By [EFG], this is approximately of order $n^{-\delta}(1 + \log \frac{n}{2})^{-3/2}$

$$\delta = 1 - \frac{1 + \log\log 2}{\log 2}.$$

The analog of Theorem 1.4 is true for the other classical groups. However, the proof requires some new results and will be proved in a sequel (where we will also give an application to probabilistic generation). We do show the following:

Theorem 1.5. *Let G be a finite classical group with natural module V of dimension n. Assume that G is defined over $\mathbb{F}_q$. Let $X(G)$ denote the union of all irreducible subgroups of G not containing the derived subgroup of G (if q is even and $G = Sp(2n,q)$, we exclude the subgroups $O^\pm(2n,q)$ from $X(G)$). Let $Y(G)$ denote the set of regular semisimple elements contained in $X(G)$.*

(1) $\lim_{n\to\infty} |Y(G)|/|G| = 0$; *and*
(2) $\lim_{\min\{n,q\}\to\infty} |X(G)|/|G| = 0$.

Luczak and Pyber [LP] proved the analog of Theorem 1.4 for symmetric and alternating groups (with irreducible replaced by transitive). Their result has been recently improved by Eberhart, Ford and Green [EFG].

Section 2 recalls bounds from our paper [FG2] on the number and sizes of conjugacy classes in finite classical groups. It also recalls needed results from the paper [FG1] on derangements in subspace actions of finite classical groups. Section 3 contains some results on Weyl groups that we require.

Section 4 proves a strengthening of the Boston-Shalev conjecture for stabilizers of imprimitive subgroups in the case of large rank. For example it shows that the proportion of elements of any coset of $SL(n,q)$ in $GL(n,q)$ which are contained in a conjugate of the wreath product $GL(m,q) \wr S_k$ goes to 0 as $n = mk \to \infty$. Moreover it is shown that the same is true for families of maximal subgroups, i.e. that the proportion of elements of any coset of $SL(n,q)$ of $GL(n,q)$ which are contained in a conjugate of $GL(m,q) \wr S_k$ for some m, k such that $mk = n$ (with $k > 1$) also goes to 0 as $n \to \infty$. This behavior is qualitatively different from the case of subspace actions. Namely it is proved in [FG1] that as $k \to \infty$, the proportion of elements fixing a k-space tends to 0. But this does *not* hold for families; the probability that a random element fixes a k space for some $1 \leq k \leq n/2$ tends to 1 as n tends to infinity.

Section 5 proves the Boston-Shalev conjecture for extension field subgroups in the case of large rank. For example it shows that the proportion of elements in a coset $gSL(n,q)$ of $GL(n,q)$ which are both regular semisimple and contained in a conjugate of $GL(n/b, q^b).b$ is at most $A/n^{1/2}$, for a universal constant A. The $.b$ notation means semidirect product with the cyclic group of order b generated by the map $x \to x^q$ on $\mathbb{F}^*_{q^b}$.

Section 6 shows how the five theorems stated in the introduction follow from earlier results (the proof of Theorem 1.4 also uses the appendix). In the appendix we use generating functions to prove a strengthening of the Boston-Shalev conjecture for GL in the case of extension field subgroups of large rank. Namely the appendix shows that the proportion of elements (not necessarily regular semisimple) in a coset $gSL(n,q)$ of $GL(n,q)$ which are contained in a conjugate of $GL(n/b, q^b).b$ goes to 0 as $n \to \infty$. The argument does not easily generalize to the other classical groups. In a follow-up paper, we use a different method to prove this strengthening (and so the analog of Theorem 1.4) for the other classical groups.

2. Background

This brief section recalls some bounds from our papers [FG1] and [FG2]. Let $k(G)$ denote the number of conjugacy classes of G. More generally, if N is a normal subgroup of G and $g \in G$, let $k(Ng)$ denote the number

of N-orbits on the coset Ng. By [FG2], $k(Ng)$ is precisely the number of g-stable conjugacy classes in N.

First note that $k(GL(n,q)) \leq q^n$ and that $k(U(n,q)) \leq 8.26q^n$ [MR].

From [FG2], we have upper bounds on the number of conjugacy classes in a finite classical group of the form cq^r where c is an explicit constant and r is the rank (indeed for the simply connected groups, one gets bounds of the form $q^r + dq^{r-1}$ for an explicit d).

TABLE 1 Class Numbers for Classical Groups

G	$k(G) \leq$	Comments
$SL(n,q)$	$2.5q^{n-1}$	
$SU(n,q)$	$8.26q^{n-1}$	
$Sp(2n,q)$	$10.8q^n$	q odd
$Sp(2n,q)$	$15.2q^n$	q even
$SO(2n+1,q)$	$7.1q^n$	q odd
$\Omega(2n+1,q)$	$7.3q^n$	q odd
$SO^{\pm}(2n,q)$	$7.5q^n$	q odd
$\Omega^{\pm}(2n,q)$	$6.8q^n$	q odd
$O^{\pm}(2n,q)$	$9.5q^n$	q odd
$SO^{\pm}(2n,q)$	$14q^n$	q even
$O^{\pm}(2n,q)$	$15q^n$	q even

Concerning centralizer sizes, the following lower bound is proved in [FG2].

Theorem 2.1. (1) *Let G be a connected simple algebraic group of rank r of adjoint type over a field of positive characteristic. Let F be a Steinberg-Lang endomorphism of G with G^F a finite Chevalley group over the field $\mathbb{F}_q$. There is an absolute constant A such that for all $x \in G^F$,*

$$|C_{G^F}(x)| > \frac{q^r}{A(1+\log_q r)}.$$

(2) *There is a universal constant A such that for all $x \in GL(n,q)$,*

$$|C_{GL(n,q)}(x)| > \frac{q^n}{A(1+\log_q n)}.$$

(3) *There is a universal constant A such that for all $x \in U(n,q)$,*

$$|C_{U(n,q)}(x)| > \frac{q^n}{A(1+\log_q n)}.$$

Regarding derangements in subspace actions of finite classical groups, we recall the following results from [FG1].

Theorem 2.2. *For $1 \leq k \leq n/2$, the proportion of elements of any coset of $SL(n,q)$ in $GL(n,q)$ which fix a k-space is at most $A/k^{.005}$, for A a universal constant.*

Theorem 2.3. *For $1 \leq k \leq n/2$, the proportion of elements of any coset of $SU(n,q)$ in $U(n,q)$ which fix a nondegenerate k-space is at most $A/k^{.005}$, for A a universal constant, and the proportion of elements of any coset of $SU(n,q)$ in $U(n,q)$ which fix a totally singular k-space is at most $A/k^{.25}$, for A a universal constant.*

Theorem 2.4. *For $1 \leq k \leq n/2$, the proportion of elements of $Sp(2n,q)$ which fix a nondegenerate $2k$ space is at most $A/k^{.005}$, for A a universal constant, and for $1 \leq k \leq n$, the proportion of elements of $Sp(2n,q)$ which fix a totally singular k-space is at most $A/k^{.25}$, for A a universal constant.*

Theorem 2.5. *For $1 \leq k \leq n/2$, the proportion of elements of $SO^{\pm}(n,q)$ which fix a nondegenerate k-space is at most $A/k^{.005}$ for A a universal constant, and the proportion of elements of $SO^{\pm}(n,q)$ which fix a totally singular k-space is at most $A/k^{.25}$, for A a universal constant.*

3. Some results on Weyl groups

We record some results about Weyl groups that will be used in Sections 4 and 5.

For $x \in S_k$, we define $\mathrm{orb}(x)$ as the number of orbits of x and $\mathrm{ind}(x) = k - \mathrm{orb}(x)$. Note that $\mathrm{ind}(x)$ is the also the minimal number d such that x is a product of d transpositions.

Lemma 3.1. *If $x \in S_k$ satisfies $\mathrm{ind}(x) < k/2$, then x fixes subsets of every size from 1 to k.*

Proof. If $k \leq 2$, then $x = 1$ and the result is clear. We may assume that $x \neq 1$. Let d be the length of the largest cycle of x. By induction, x fixes subsets of every size at most $k-d$. If $d \leq k/2$, then the result follows (since it is enough to check subsets of size up to $k/2$). If $d > k/2$, then it follows that x is a d-cycle with $d = (k+1)/2$ (in particular, k is odd). Thus, x has $(k-1)/2$ fixed points and again the result is clear. □

To see that Lemma 3.1 is sharp, note that a fixed point free involution $x \in S_k$ fixes no subsets of odd size and also satisfies $\mathrm{ind}(x) = k/2$.

Lemma 3.2. *For $0 < t < 1$, and $r \geq 1$, the coefficient of u^r in $(1-u)^{-t}$ is at most $te^t r^{t-1}$.*

Proof. This coefficient is equal to $\frac{t}{r}\prod_{i=1}^{r-1}(1+\frac{t}{i})$. Taking logarithms base e, one sees that

$$\begin{aligned} \log\left[\prod_{i=1}^{r-1}\left(1+\frac{t}{i}\right)\right] &= \sum_{i=1}^{r-1}\log\left(1+\frac{t}{i}\right) \\ &\leq \sum_{i=1}^{r-1}\frac{t}{i} \\ &\leq t(1+\log(r-1)). \end{aligned}$$

Taking exponentials one sees that the sought proportion is at most $te^t r^{t-1}$. □

Lemma 3.3. *For $b|n$, the proportion of elements in S_n all of whose cycles have length divisible by b is at most $1.2/n^{1-1/b}$.*

Proof. By the cycle index of the symmetric groups (reviewed in the prequel [FG1]), the sought proportion is the coefficient of u^n in

$$\prod_{i\geq 1} e^{\frac{u^{ib}}{ib}} = (1-u^b)^{-1/b}.$$

Now apply Lemma 3.2 with $r = n/b$ and $t = 1/b$ to get an upper bound of

$$\frac{e^{1/b}}{b^{1/b} n^{1-1/b}} \leq 1.2/n^{1-1/b}.$$

□

Corollary 3.4. *The proportion of elements in S_n with all cycle lengths divisible by some prime b is at most $A/n^{1/2}$ for some universal constant A.*

Proof. It follows from Lemma 3.3 that the sought proportion is at most

$$1.2 \sum_{b|n} \frac{1}{n^{1-1/b}},$$

where the sum is over prime divisors b of n. Since n has at most $\log_2(n)$ distinct prime factors, this is at most

$$\frac{1.2}{n^{1/2}} \left[1 + \frac{\log_2(n)}{n^{1/6}}\right],$$

and the result follows. □

We conclude this section with a result about signed permutations.

Lemma 3.5. *Let $W = B_n$ be the Weyl group of type B. The proportion of elements in W such that all odd cycles have a given type and all even cycles have a given type is at most $\frac{1}{\sqrt{\pi n}}$.*

Proof. We prove the lemma in the case that all even cycles have positive type, and all odd cycles have negative type; the other cases are similar. As in [FG1], we apply the cycle index of the groups B_n. For a signed permutation π, let $n_i(\pi)$ denote the number of positive i-cycles of π, and let $m_i(\pi)$ denote the number of negative i-cycles of π. The cycle index states that

$$1 + \sum_{n\geq 1} \frac{u^n}{2^n n!} \sum_{\pi \in B_n} \prod_i x_i^{n_i(\pi)} y_i^{m_i(\pi)} = \prod_{i\geq 1} e^{u^i (x_i + y_i)/(2i)}.$$

Setting

$$x_1 = x_3 = x_5 = \cdots = 0, \quad y_2 = y_4 = y_6 = \cdots = 0,$$
$$x_2 = x_4 = x_6 = \cdots = 1, \quad y_1 = y_3 = y_5 = \cdots = 1,$$

gives that the proportion of elements of W with all even cycles positive and all odd cycles negative is the coefficient of u^n in

$$\prod_{i \geq 1} e^{u^i/(2i)} = (1-u)^{-1/2}.$$

Arguing as in [FG1] shows that this proportion is at most $\frac{1}{\sqrt{\pi n}}$. □

4. Stabilizers of imprimitive subgroups

This section proves a strengthening of the Boston-Shalev conjecture for wreath products when the rank $n \to \infty$.

Subsection 4.1 develops some preliminaries for the wreath product case. Subsections 4.2, 4.3, 4.4, and 4.5 treat wreath products for the general linear, unitary, symplectic, and orthogonal groups respectively. Subsection 4.6 considers stabilizers for pairs of totally isotropic subspaces.

4.1. **Preliminaries for wreath products.** Let $p(n)$ denote the number of partitions of an integer n; this is equal to the number of conjugacy classes of S_n. The series $p(n)$ begins with 1,2,3,5,7,11,15,22. Lemma 4.1, proven in the textbook [VW], gives a useful upper bound on $p(n)$.

Lemma 4.1. *Let $p(n)$ be the number of partitions of n. For $n \geq 2$,*

$$p(n) \leq \frac{\pi}{\sqrt{6(n-1)}} e^{\pi\sqrt{2n/3}}.$$

Remark: Hardy and Ramanujan [HR] give an elementary proof that $p(n) < \frac{K}{n} e^{2\sqrt{2n}}$ for a universal constant K. In truth $p(n)$ is asymptotic to $\frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}$, as discussed in [An].

Next we recall a description (proved in [JK]) of conjugacy classes of the wreath product $G \wr S_k$, where G is any finite group. The classes are parameterized by matrices where

(1) The rows are indexed by conjugacy classes of G.
(2) The number of columns is k.
(3) Letting $a_{h,i}$ denote the (h,i) entry of the matrix, the $a_{h,i}$ are non-negative integers satisfying $\sum_{h,i \geq 1} i \cdot a_{h,i} = k$.

To determine the data corresponding to an element $(g_1, \cdots, g_k; \pi)$ in the wreath product, to each i-cycle of π one associates a conjugacy class C of G by multiplying (in the order indicated by the cycle of π) the g's whose subscripts form the entries of the cycle of π and letting C be the conjugacy class in G of the resulting product. This contributes 1 to the entry of the matrix whose row entry is indexed by C and whose column number is i.

Lemma 4.2. *Suppose that $n > 1$.*

(1) *Let $W(B_n)$ be the Weyl group of type B_n. Then*

$$k(W(B_n)) \leq \frac{(n+1)\pi^2}{6(n-1)} e^{2\pi\sqrt{2n/3}}.$$

(2) *Let $W(D_n)$ be the Weyl group of type D_n. Then*

$$k(W(D_n)) \leq \frac{(n+1)\pi^2}{3(n-1)} e^{2\pi\sqrt{2n/3}}.$$

Proof. Since $[W(B_n) : W(D_n)] = 2$, (2) follows from (1).

By the above description of conjugacy classes of wreath products, the conjugacy classes of $W(B_n)$ are indexed by pairs of partitions (α, β) where α is a partition of a and β is a partition of $n-a$ for $0 \leq a \leq n$. It follows that $k(W(B_n)) \leq (n+1)k(S_n)^2$ and so by Lemma 4.1,

$$k(W(B_n)) \leq \frac{(n+1)\pi^2}{6(n-1)} e^{2\pi\sqrt{2n/3}}.$$

□

Next we proceed to the main results of this section.

4.2. **GL(n,q).** To begin we consider cosets of $SL(n,q)$ in $GL(n,q)$, with q fixed and $n \to \infty$. We note that Theorem 4.3 was proved by Shalev [Sh] for q fixed by using deep work of Schmutz [Sc] on the order of a random matrix. Our method is more elementary and extends to the other finite classical groups.

Theorem 4.3. *There exist positive constants B and δ so that the following holds (independently of n, q, m). Let $n = mk$ and let $G = GL(n,q)$. Set $H = GL(m,q) \wr S_k$. The proportion of elements of G in a coset of $SL(n,q)$ which are conjugate to an element of H is less than B/n^δ.*

Recall [HWr, Theorem 315] that $d(n)$, the number of divisors of n, decays faster than any power of n. Thus, the conclusion of the theorem holds allowing all possible m, k.

Proof. Let $H_0 = GL(m,q) \times \ldots \times GL(m,q)$, where there are k copies of $GL(m,q)$. Consider cosets of the form xH_0 where $x \in S_k$ and $\mathrm{ind}(x) \geq k/2$. Recall that $k(GL(m,q)) \leq q^m$. By the description of conjugacy classes in a wreath product in the previous subsection, the number of H_0 orbits on the coset xH_0 is $k(GL(m,q))^{\mathrm{orb}(x)} \leq q^{n/2}$. Thus the total number of G-conjugacy classes intersecting xH_0 for any such x is at most

$$p(k)q^{n/2} \leq \frac{\pi}{\sqrt{6(k-1)}} e^{\pi\sqrt{2k/3}} q^{n/2}.$$

Here $p(k)$ denotes the number of partitions of k and we have used Lemma 4.1.

Using the estimate for the smallest centralizer size (Lemma 2.1) gives that the proportion of elements of G conjugate to some such element xH_0 is at most (for a universal constant A)

$$\frac{\pi}{\sqrt{6(k-1)}} e^{\pi\sqrt{2k/3}} A(1+\log_q n)/q^{n/2} < B/n^\delta.$$

Even after multiplying by $q-1$, we still have the same estimate giving the result for each coset.

Now consider cosets xH_0 where $\mathrm{ind}(x) < k/2$. By Lemma 3.1 x fixes subsets of every possible size and so any element in xH_0 fixes a subspace of dimension $n/2$ (for k even) and $(k-1)m/2$ (for k odd). In particular, every such element fixes a d dimensional space for some fixed $d \geq n/4$. By Theorem 2.2, it follows that the proportion of elements in a given coset of $SL(n,q)$ which fix a subspace of that dimension is at most $C/(n/4)^{.005}$ and the result follows. □

4.3. **U(n,q).** Using the same method as in the general linear case, one establishes analogous results for the unitary groups. The proof here requires a little extra effort since we only have the bound $k(U(m,q)) < 8.3q^m$.

Theorem 4.4. *There exist positive constants B and δ so that the following holds (independently of n,q,m). Let $n = mk$ and let $G = U(n,q)$. Set $H = U(m,q) \wr S_k$. The proportion of elements of G in a coset of $SU(n,q)$ which are conjugate to an element of H is less than B/n^{δ}. The same is true allowing all possible m.*

Proof. As for GL, the second statement follows from the first by [HWr]. Set $H_0 = U(m,q) \times \ldots \times U(m,q)$. The proof is precisely along the lines of the GL case. The only difference is that we have to use the estimate $k(U(m,q)) < 8.3q^m$. We first consider cosets xH_0 where $x \in S_k$ and $\mathrm{ind}(x) \geq k/2$. The argument then gives the estimate that the proportion of elements of G conjugate to an element in xH_0 for some such x is at most

$$\frac{\pi}{\sqrt{6(k-1)}} e^{\pi\sqrt{2k/3}} (8.3)^{k/2} A(1+\log_q n)/q^{n/2} < B/n^{\delta}.$$

This estimate is valid (even multiplying by $q+1$) is valid as long as q^m is bigger than 8.3. This holds unless $m=1$ or $m=2=q$ or $m=3$ and $q=2$. If $m=1$, we use the fact that $k(U(1,q)) = q+1 \leq (3/2)q$ and since $3/2 < 2 \leq q$, the proof goes through. If $m=2=q$, the same estimate holds (alternatively we note that if $m=2=q$, our subgroup H is contained in $U(1,2) \wr S_n$). Similarly, if $m=3$ and $q=2$, then $k(U(3,2)) = 24 < 3^3$ (and H is again contained in $U(1,2) \wr S_n$). Again, multiplying by $q+1$ shows the same estimate holds for each coset.

Now consider cosets xH_0 where $x \in S_k$ and $\mathrm{ind}(x) < k/2$. Arguing as for GL shows that any element in xH_0 fixes a nondegenerate subspace of fixed dimension at least $n/4$. Now apply Theorem 2.3 to obtain the result. □

4.4. **Sp(2n,q).** One has the following result (Theorem 4.5), proven the same way as Theorems 4.3 and 4.4. We use the bound $k(Sp(2m,q)) \leq 15.2q^m$. Note that $k(Sp(2,q)) \leq (3/2)q$ for q even and $k(Sp(2,q)) \leq (7/3)q$ for q odd. Similarly $k(Sp(4,q)) \leq (11/4)q^2$ for q even and $k(Sp(4,q)) \leq (34/9)q^2$ for q odd. We also have that $k(Sp(6,2)) = 30 = (15/4)2^3$. We use these

estimates, all of which follow from the generating functions for $k(Sp)$ in [FG2].

Theorem 4.5. *There exist positive constants B and δ so that the following holds (independently of n, q, m). Let $n = mk$ and let $G = Sp(2n, q)$. Set $H = Sp(2m, q) \wr S_k$. The proportion of elements in G which are conjugate to an element of H is less than B/n^δ. The same is true allowing all possible m.*

Proof. The last statement follows from the first by [HWr]. Let H_0 be the subgroup $Sp(2m, q) \times \ldots \times Sp(2m, q)$.

Arguing as for the unitary groups, we see that the proportion of elements of G conjugate to an element in some coset xH_0 with $x \in S_k$ and $\mathrm{ind}(x) \geq k/2$ is at most

$$\frac{\pi}{\sqrt{6(k-1)}} e^{\pi\sqrt{2k/3}} (15.2)^{k/2} A(1 + \log_q n)/q^{n/2}.$$

This is clearly at most B/n^δ unless possibly $m = 1$ and $q < 16$ or $m = 2$ and $q < 4$ or $m = 3$ and $q = 2$. Replacing the 15.2 by the better estimates noted before the proof shows that the estimate still is valid in these cases.

The bound for elements conjugate to a coset in xH_0 for $\mathrm{ind}(x) < k/2$ follows precisely as in the GL or U case. □

4.5. $\Omega(n, q)$**.** Finally, we consider orthogonal groups. The proof is quite similar but there is one easy extra case to consider. We prove the result for $SO^\pm(n, q)$ (which implies the result for Ω).

Let $X = O^\pm(n, q) = O(V)$ and $G = SO^\pm(n, q) = SO(V)$. Assume that $n > 6$ and that if q is even, then n is even. Write $V = V_1 \perp \ldots \perp V_k$, $k > 1$ where the V_i are nondegenerate spaces of the same type. Let H denote the stabilizer of this decomposition in X. Thus, $H \cong O(m, q) \wr S_k$ (the possibilities for the type of V_i depend upon k and the type of V). Set $H_0 = O(m, q) \times \ldots \times O(m, q)$.

We first consider the case that $m = 1$ and q is odd (if q is even, then the stabilizer of an additive decomposition of nondegenerate 1-spaces is not irreducible and in particular not maximal). Note that in this case H is the Weyl group of type B_n and so is isomorphic to $\mathbb{Z}/2 \wr S_n$. The intersection of H with $SO^\pm(n, q)$ will be the Weyl group of type D_n. By Lemma 4.2, the number of conjugacy classes of $SO^\pm(n, q)$ that intersect H is at most

$$\frac{(n+1)\pi^2}{3(n-1)} e^{2\pi\sqrt{2n/3}}.$$

Thus, by Theorem 2.1, the proportion of elements of $SO^\pm(n, q)$ that intersect H is at most

$$A(1 + \log_q r) \frac{(n+1)\pi^2}{3(n-1)} e^{2\pi\sqrt{2n/3}}/q^r,$$

where $r = n/2$ if n is even and $r = (n-1)/2$ for n odd. This is less than B/n^δ for a universal B and δ.

If $m > 1$, the identical proof for the case of symplectic (or unitary) groups goes through. Note that we have a slightly better inequality for $k(O(m,q))$ than in the symplectic case. Note that if q is even, m is also even (because any odd dimensional space has a radical and so the stabilizer of such a decomposition is not irreducible). The only additional wrinkle in the proof is that we are working with $H \cap SO^{\pm}(n,q)$ and so when estimating the number of classes in a given coset xH, we may have to multiply by 2. This is absorbed in the the constant for the size of the centralizer and so causes no problems.

Thus, we have:

Theorem 4.6. *There exist positive constants B and δ so that the following holds (independently of n, q, m). Let $n = mk$ and let $G = SO^{\pm}(n,q)$. Set $H = SO^{\pm}(n,q) \cap [O^{\pm}(m,q) \wr S_k]$. If q is even, assume that both n and m are even. For n sufficiently large, the proportion of elements in G which are conjugate to an element of H is less than B/n^{δ}. The same is true allowing all permissible m.*

4.6. **Stabilizers of pairs of totally isotropic subspaces.** We consider imprimitive subgroups permuting a direct sum decomposition of totally isotropic spaces. Note that if there are more than 2, we would be contained in the stabilizer of an additive decomposition of nondegenerate spaces (by taking pairs of the totally singular subspaces). See [As] for the description of the maximal subgroups of the classical groups.

To begin, we treat the case of $GL(n,q^2).2$ in $U(2n,q)$.

Theorem 4.7. *There exist absolute positive constants B and δ so that for n sufficiently large, the proportion of elements of $U(2n,q)$ contained in a conjugate of $H := GL(n,q^2).2$ is at most B/n^{δ}.*

Proof. If an element of $U(2n,q)$ is contained in $GL(n,q^2)$, then it fixes a totally singular n-dimensional space. By Theorem 2.3, the proportion of such elements tends to 0 at the correct rate.

By Shintani descent ([FG2]), the H-conjugacy classes in the nontrivial coset of $GL(n,q^2)$ correspond exactly to conjugacy classes of $U(n,q)$. The number of conjugacy classes of $U(n,q)$ is at most $8.26q^n$. In particular, the number of $U(2n,q)$-classes in the nontrivial coset is at most $8.26q^n$. Theorem 2.1 gives an upper bound for the size of a conjugacy class of $U(2n,q)$. It follows that the proportion of elements of $U(2n,q)$ conjugate to an element of the nontrivial coset of $GL(n,q^2)$ is at most

$$8.26q^n \frac{A(1+\log_q(2n))}{q^{2n}},$$

where A is a universal constant. This is much smaller than B/n^{δ}. □

A minor variant of the proof gives the following:

Theorem 4.8. *The proportion of elements of in any coset of $SU(2n,q)$ in $U(2n,q)$ contained in a conjugate of $H := GL(n,q^2).2$ tends to 0 as $n \to \infty$, uniformly in q.*

To treat the case of $GL(n,q).2$ inside of $Sp(2n,q)$ or $SO(2n,q)$, the following lemma will be helpful. See also Lemma 5.10 for a related result about unitary groups.

Lemma 4.9. *Let $G^+(n,q)$ denote the extension of $GL(n,q)$ generated by the inverse transpose involution τ, and let $k(GL(n,q)\tau)$ be the number of $G^+(n,q)$ conjugacy classes in the coset $GL(n,q)\tau$.*

1. *$k(GL(n,q)\tau)$ is the number of real conjugacy classes of $GL(n,q)$; and*
2. *$k(GL(n,q)\tau) \leq 28q^{\lfloor n/2 \rfloor}$;*
3. *The number of real conjugacy classes in $GL(n,q)$ is at most $28q^{\lfloor n/2 \rfloor}$.*

Proof. By [FG2], the number of $G^+(n,q)$ classes in the outer coset is precisely the number of $GL(n,q)$ classes that are invariant under the involution. Since any element of $GL(n,q)$ is conjugate to its transpose, the τ invariant classes of $GL(n,q)$ are precisely the real classes, whence the first statement holds. The second statement follows from the upper bound on $k(GL(n,q)\tau)$ in [FG3]. The final statement is now clear. □

Theorem 4.10. *There exist absolute positive constants B and δ so that the following hold for n sufficiently large.*

1. *The proportion of elements of $Sp(2n,q)$ contained in a conjugate of $GL(n,q).2$ is at most B/n^{δ}.*
2. *The proportion of elements of $SO^+(2n,q)$ contained in a conjugate of $GL(n,q).2$ is at most B/n^{δ}.*

Proof. As the argument is the same for both parts, we give details for the first part. Note that if an element of $Sp(2n,q)$ is conjugate to an element of $GL(n,q)$, then it fixes a totally singular n-space. By Theorem 2.4, the proportion of such elements is at most $B/n^{.25}$.

By Lemma 4.9, the number of $GL(n,q)$ classes in the outer coset in $GL(n,q).2$ is at most $28q^{\lfloor n/2 \rfloor}$. By Theorem 2.1, any conjugacy class of $Sp(2n,q)$ has size at most

$$\frac{A(1+\log_q(n))|Sp(2n,q)|}{q^n},$$

which implies the result. □

5. Extension field subgroups

This section analyzes extension field subgroups in the case where the rank approaches infinity. The standard extension field cases for the groups GL, U, Sp, O are treated in Subsections 5.1, 5.2, 5.3, and 5.4 respectively.

Subsection 5.5 considers some special cases, namely $U(n,q).2$ in $Sp(2n,q)$ and $U(n,q).2$ in $SO^{\pm}(2n,q)$.

First we consider an example which shows that the bounds cannot be improved too much.

Example 5.1. *Let $n = 2m$ be a positive integer. Set $G = GL(n,q)$ and consider $H = GL(m,q^2) < G$. Fix m and let q grow. Then almost all elements of H are regular semisimple (even in G). Let X be the set of elements in S_n in which all cycles have even length. We see that H contains conjugates of any maximal tori T_w of G where $w \in X$. It follows that*

$$\lim_{q\to\infty} |\cup_{g\in G, w\in X} gT_w g^{-1}| = |X|/n!.$$

From [FG1], *$|X|/n!$ is asymptotic to $\sqrt{\frac{2}{\pi n}}$. Thus, the proportion of derangements in the action of G on $N_G(H)$ is of order $n^{-1/2}$ for q large.*

One can construct a similar example with n increasing by letting q increase very rapidly.

5.1. **GL(n,q).** Recall that $GL(n/b,q^b).b$ denotes the semidirect product of $GL(n/b,q^b)$ with the cyclic group of order b generated by the map $x \to x^q$ on $\mathbb{F}^*_{q^b}$; this group is maximal when b is prime [As]. The main result of this subsection is that the proportion of elements in a given coset of $SL(n,q)$ in $GL(n,q)$ which are both regular semisimple and contained in a conjugate of $GL(n/b,q^b).b$ is at most $A/n^{1/2}$ for a universal constant A. A stronger result (requiring a more intricate proof) is in the appendix.

Theorem 5.2. *Let b be prime. The number of $GL(n,q)$ classes of the group $GL(n/b,q^b).b$ outside $GL(n/b,q^b)$ is at most $(b-1)q^{n/b} \leq 2q^{n/2}$.*

Proof. Let H denote $GL(n/b,q^b).b$. Fix a generator of the subgroup of order b, say x with x inducing the q-Frobenius map on $H_0 = GL(n/b,q^b)$.

Fix $0 < i < b$. By Shintani descent, there is a bijection between H-conjugacy classes in the coset H_0x^i and conjugacy classes in $GL(n/b,q)$. So there are at most $(b-1)q^{n/b}$ conjugacy classes in $H \setminus H_0$. This is easily seen to be at most $2q^{n/2}$. □

This result is sufficient to prove the Boston–Shalev result for $SL(n,q)$.

Corollary 5.3. *Let $n \geq 3$. Let b be a prime dividing n. There is a universal constant B such that the proportion of elements in $G := SL(n,q)$ which are contained in a conjugate of $H := GL(n/b,q^b).b$ is at most*

$$\frac{1}{b} + \frac{B(1+\log_q n)}{q^{n/2-1}}.$$

Proof. By the previous result, there are at most $2q^{n/2}$ conjugacy classes of $GL(n,q)$ that intersect $H \setminus H_0$ where $H_0 = GL(n/b,q^b)$. By Theorem 2.1,

this implies that the proportion of elements of $GL(n,q)$ which intersect some conjugate of $H \setminus H_0$ is at most

$$\frac{B(1+\log_q n)}{q^{n/2}}$$

for some universal constant B. Thus, the proportion of elements of G contained in a conjugate of of $H \setminus H_0$ is at most $B'(1+\log_q n)/q^{n/2-1}$.

Since $[N_G(H_0) : H_0] = b$, it follows that the union of the conjugates of H_0 contains at most $|G|/b$ elements, whence the result. □

We now get some better estimates at least for q large.

Lemma 5.4. *Let b be a prime divisor of n. If an element of $GL(n,q)$ is contained in a conjugate of $GL(n/b,q^b)$, then every irreducible factor of its characteristic polynomial either has degree divisible by b or has every Jordan block size occur with multiplicity a multiple of b.*

Proof. Consider an element $A \in GL(n/b,q^b)$. We can write A as a block diagonal matrix where the block diagonals are of the form $C_{p_i} \otimes J_i$ where C_{p_i} is the companion matrix of the irreducible polynomial $p_i \in \mathbb{F}_{q^b}[x]$ and J_i is a regular unipotent matrix of the appropriate size.

Since b is prime, there are two possibilities for p_i. The first is that p_i is defined over $\mathbb{F}_q$ (and is of course irreducible over $\mathbb{F}_q$). The second is that p_i has b distinct Galois conjugates over $\mathbb{F}_q$ so the product of these conjugates f_i is defined and irreducible over $\mathbb{F}_q$. This proves the lemma. □

Now we proceed to the main result of this subsection.

Theorem 5.5. *Let b be a prime dividing n with $n \geq 3$.*

1. *The proportion of elements in a coset $gSL(n,q)$ in $GL(n,q)$ which are regular semisimple and contained in a conjugate of $GL(n/b,q^b).b$ is at most $A/n^{1/2}$ for a universal constant A.*
2. *The proportion of elements in a coset $gSL(n,q)$ in $GL(n,q)$ which are regular semisimple and contained in a conjugate of $GL(n/b,q^b).b$ for some prime b is at most $A/n^{1/2}$ for a universal constant A.*

Proof. We argue exactly as in the proof of Corollary 5.3 to see that the proportion of elements in a coset $gSL(n,q)$ contained in a conjugate of $GL(n/b,q^b).b \setminus GL(n/b,q^b)$ is at most

$$\frac{B(1+\log_q n)}{q^{n/2-1}}$$

for some universal constant B. Summing over all possible b just multiplies the upper bound by at most $\log_2(n)$ (since there are most $\log_2(n)$ possibilities for b). This is still much less than $A/n^{1/2}$. Note we are not restricting to semisimple regular elements in this case.

Now we consider semisimple regular elements in a coset $gSL(n,q)$ contained in some conjugate of $GL(n,q^b)$. By Lemma 5.4, any such element

has characteristic polynomial a product of polynomials with all irreducible factors having degree a multiple of b. Thus, any such element is contained in a maximal torus T_w with $w \in S_n$ and all cycles lengths of w being a multiple of b. By Corollary 3.4, the proportion of $w \in S_n$ with that property is at most $A/n^{1/2}$ for a universal constant A. Arguing as in [FG1, §5], this implies that the proportion of regular semisimple elements in $gSL(n,q)$ with this property is also at most $A/n^{1/2}$.

Combining these two estimates proves (2) (and also (1)).

□

5.2. **U(n,q).** To begin we have the following unitary analog of Theorem 5.2.

Theorem 5.6. *Let b be an odd prime. Then the number of $U(n,q)$ classes in $U(n/b,q^b).b$ outside $U(n/b,q^b)$ is at most $(b-1)k(U(n/b,q))$.*

Proof. Set $H = U(n/b,q^b).b$ and $H_0 = U(n/b,q^b)$. By Shintani descent, the number of H-conjugacy classes in any nontrivial coset of H_0 is $k(U(n/b,q))$, whence the result. □

The Boston–Shalev result follows in this case arguing precisely as in Corollary 5.3. It also follows from our results below.

The following theorem is the main result of this subsection.

Theorem 5.7. *Let b be an odd prime dividing n.*

1. *The proportion of elements in a coset $gSU(n,q)$ in $U(n,q)$ which are both regular semisimple and contained in a conjugate of $U(n/b,q^b).b$ is at most $A/n^{1/2}$ for a universal constant A.*
2. *The proportion of elements in a coset $gSU(n,q)$ in $U(n,q)$ which are both regular semisimple and contained in a conjugate of $U(n/b,q^b).b$ for some odd prime b is at most $A/n^{1/2}$ for a universal constant A.*

Proof. The proportion of elements in $gSU(n,q)$ contained in a conjugate of $U(n/b,q^b).b \setminus U(n/b,q^b)$ is at most

$$(b-1)k(U(n/b,q))B(1+\log_q n)(q+1)/q^n,$$

for some universal constant (by Theorem 5.6 and Theorem 2.1). Since $k(U(n/b,q)) \leq 8.3q^{n/b}$, the result holds for these elements.

Next consider the proportion of regular semisimple elements in $gSU(n,q)$ contained in a conjugate of $U(n/b,q^b)$. Any regular semisimple element of $U(n,q)$ contained in a conjugate of $U(n/b,q^b)$ is a contained in a maximal torus of the latter group. These are also maximal tori of the larger group and correspond to T_w with $w \in S_n$ the Weyl group of $U(n,q)$, where all cycles of w have length divisible by b (by precisely the same argument as for GL).

By [FG1, §5] and Corollary 3.4, the proportion of such elements (summing over all b) is at most $B'/n^{1/2}$ for some absolute constant B'. Thus (2) and so also (1) hold. □

5.3. **Sp(2n,q).** This subsection analyzes the case of the symplectic groups.

Theorem 5.8. *Let b be a prime dividing n.*

(1) *The proportion of elements in $Sp(2n,q)$ which are regular semisimple and contained in a conjugate of $Sp(2n/b,q^b).b$ is at most $\frac{A}{n^{1/2}}$ where A is a universal constant.*
(2) *The proportion of elements in $Sp(2n,q)$ which are regular semisimple and contained in a conjugate of $Sp(2n/b,q^b).b$ for some prime $b|n$ is at most $\frac{A}{n^{1/2}}$ where A is a universal constant.*

Proof. We will prove (2). Then (1) follows immediately.

As usual, by Shintani descent, the number of $Sp(2n/b,q^b).b$ classes in an outer class is at most $(b-1)k(Sp(2n/b,q)) < 15.2(b-1)q^{n/b}$. By Theorem 2.1, the estimate easily holds for such elements (summing over all prime divisors b of n).

Now consider the conjugates of $Sp(2n/b,q^b)$. By the argument for the GL case, we see that every factor of the characteristic polynomial of a regular semisimple element g in $Sp(2n/b,q^b)$ has degree divisible by b. Moreover, the centralizer of g is contained in $Sp(2n/b,q^b)$. Thus any element in $Sp(2n/b,q^b)$ is contained in a conjugate of a maximal torus T_w where w is in the Weyl group and has all cycles of length divisible by b. By Corollary 3.4 and [FG1, §5], it follows that the proportion of regular semisimple elements conjugate to an element of $Sp(2n/b,q^b)$ is at most $D/n^{1/2}$ for some constant D. This gives the result. □

5.4. **O(n,q).** The proof for SO is essentially identical to that of Sp. The only difference in the argument is to use strongly regular semisimple elements (i.e. semisimple elements whose characteristic polynomials have distinct roots). Note that if b is odd, then the two orthogonal groups will have the same type. If $b=2$, then the big group must have + type.

Theorem 5.9. (1) *For a prime number $b|n$, the proportion of elements in $SO^{\pm}(2n,q)$ which are both strongly regular semisimple and contained in a conjugate of $SO^{\pm}(2n/b,q^b).b$ is at most $\frac{A}{n^{1/2}}$ where A is a universal constant.*
(2) *The proportion of elements in $SO^{\pm}(2n,q)$ which are both strongly semisimple regular and contained in a conjugate of $SO^{\pm}(2n/b,q^b).b$ for some prime $b|n$ is at most $\frac{A}{n^{1/2}}$ where A is a universal constant.*

5.5. **Some special cases.** In this subsection, we treat some special cases of extension field groups.

To begin we treat the case of $U(n,q).2$ contained in $Sp(2n,q)$ (recall that $U(n,q)$ is contained in $GL(n,q^2)$ and imbeds in $Sp(2n,q)$ via the embedding of $GL(n,q^2)$ in $GL(2n,q)$).

Lemma 5.10 upper bounds the number of real conjugacy classes of $U(n,q)$.

Lemma 5.10. *The number of real conjugacy classes of $U(n,q)$ is equal to the number of real conjugacy classes of $GL(n,q)$ and is at most $28q^{\lfloor n/2 \rfloor}$.*

Proof. Let C be a conjugacy class of $U(n,q)$. Let $\bar{C}$ denote the corresponding conjugacy class in the algebraic group $GL(n,\bar{\mathbb{F}}_q)$. Note that since all centralizers in $GL(n,\bar{\mathbb{F}}_q)$ are connected, $\bar{C} \cap U(n,q)$ and $\bar{C} \cap GL(n,q)$ are single conjugacy classes in the corresponding finite group (by Lang's theorem).

Note that if $C = C^{-1}$, then C is invariant under the q-Frobenius map and so has a representative in $GL(n,q)$ and conversely. Thus, the map $C \to \bar{C} \cap GL(n,q)$ gives a bijection between real classes of $GL(n,q)$ and $U(n,q)$. The result now follows by Lemma 4.9. □

Theorem 5.11. *The proportion of elements of $Sp(2n,q)$ that are regular semisimple and conjugate to an element of $U(n,q).2$ is at most $\frac{A}{n^{1/2}}$ for a universal constant A.*

Proof. First consider classes of $Sp(2n,q)$ in the nontrivial coset of $U(n,q)$. The number of $U(n,q)$ orbits on this coset is precisely the number of conjugacy classes of $U(n,q)$ which are left invariant by the outer automorphism. It is a straightforward exercise to see that all such classes are real in $U(n,q)$. Thus, by Lemma 5.10, the number of them is at most $28q^{\lfloor n/2 \rfloor}$. Using Theorem 2.1 to upper bound the size of a conjugacy classes of $Sp(2n,q)$, it follows that the proportion of elements of $Sp(2n,q)$ conjugate to an element in the non-trivial coset of $U(n,q)$ is at most

$$\frac{q^{n/2} C(1 + \log_q(n))}{q^n},$$

for a universal constant C, whence the result holds for such elements.

If $g \in Sp(2n,q)$ is a regular semsimple element conjugate to an element of $U(n,q)$, then g is certainly regular semisimple in $U(n,q)$ and so is contained in some maximal torus T of $U(n,q)$. Since $U(n,q)$ and $Sp(2n,q)$ are both rank n groups, T is also a maximal torus of $Sp(2n,q)$. By considering the embedding of the maximal torus, we see that T is conjugate to a maximal torus T_w where w is the Weyl group (of type B) and all odd cycles have $-$ type and all even cycles have $+$ type. By Lemma 3.5, and [FG1, §5], it follows that the proportion of elements which are both regular semisimple and conjugate to an element of $U(n,q)$ is at most $C'/n^{1/2}$ for a universal constant C'. The result follows. □

The identical proof works for SO (noting that the Weyl group of type D is a subgroup of index 2 in the Weyl group of type B) and using strongly regular semisimple elements rather than semisimple regular elements.

Theorem 5.12. *The proportion of elements of $SO^{\pm}(2n,q)$ that are strongly regular semisimple and conjugate to an element of $U(n,q).2$ is at most $\frac{A}{n^{1/2}}$ for a universal constant A.*

6. Proofs of the theorems

Theorems 1.3 and 1.5 follow immediately by the results of Sections 4 and 5. Theorem 1.4 also uses the appendix.

Note that the results of Sections 4 and 5 show that for the maximal imprimitive groups and the extension field groups, the proportion of elements which are both regular semisimple (or strongly regular semisimple for the orthogonal groups) and are not derangements (for at least one of the actions) goes to 0 with n. Since the proportion of regular semisimple elements (or strongly regular semisimple elements) is greater than .016 [FNP], the proportion of regular semisimple elements which are derangements in all such actions is at least .016 (for n sufficiently large). Combining this result with the main results of [FG1, FG2, FG4] yields Theorem 1.2. Theorem 1.2 and the results of [LP] on symmetric groups yield Theorem 1.1.

References

[An] Andrews, G., *The theory of partitions*, Addison-Wesley, Reading, Mass., 1976.

[As] Aschbacher, M., On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

[BDF] Boston, N., Dabrowski, W., Foguel, T., et al., The proportion of fixed-point-free elements in a transitive permutation group, *Comm. Algebra* **21** (1993), 3259-3275.

[CC] Cameron, P. J. and Cohen, A. M., On the number of fixed point free elements in a permutation group, *Discrete Math.* **106/107** (1992), 135–138.

[DFG] Diaconis, P., Fulman, J., and Guralnick, R., On fixed points of permutations, *J. Algebraic Combin.* **28** (2008), 189-218.

[EFG] Eberhard, S., Ford, K., and Green, B., Permutations fixing a k-set, Arxiv 1507.04465 (2015).

[F] Fulman, J., Cycle indices for the finite classical groups, *J. Group Theory* **2** (1999), 251–289.

[FG1] Fulman, J. and Guralnick, R., Derangements in subspace actions of finite classical groups, to appear in *Trans. Amer. Math. Soc.*

[FG2] Fulman, J. and Guralnick, R., Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), 3023-3070.

[FG3] Fulman, J. and Guralnick, R., Conjugacy class properties of the extension of $GL(n, q)$ generated by the inverse transpose involution, *J. Algebra* **275** (2004), 356-396.

[FG4] Fulman, J. and Guralnick, R., Derangements in simple and primitive groups, in *Groups, combinatorics & geometry (Durham, 2001)*, 99-121, World Sci. Publ., River Edge, NJ, 2003.

[FNP] Fulman, J., Neumann, P.M. and Praeger, C.E., A generating function approach to the enumeration of matrices in finite classical groups, *Mem. Amer. Math. Soc.* **176** (2005), no. 830, vi+90 pp.

[GL] Guralnick, R. and Lübeck, F., On p-singular elements in Chevalley groups in characteristic p, *Groups and Computation III*, Ohio State Univ. Math. Res. Inst. Publ. 8, (2001), 170-182.

[GM] Guralnick, R. and Malle, G., Simple groups admit Beauville structures, *J. Lond. Math. Soc.* **85** (2012), 694–721.

[HR] Hardy, G.H. and Ramanujan, S., Asymptotic formulae in combinatory analysis, *Proc. Londom Math. Soc.* **17** (1918), 75-115.

[HWr] Hardy, G.H. and Wright, E.M., *An introduction to the theory of numbers*. Fifth Edition. Clarendon Press. Oxford, 1979.

[JK] James, G. and Kerber, A., *The representation theory of the symmetric group*. Encyclopedia of Mathematics and its Applications, 16. Addison-Wesley Publishing Co., Reading, Mass., 1981.

[LP] Luczak, T., and Pyber, L., On random generation of the symmetric group, *Combin. Probab. and Computing* **2** (1993), 505-512.

[M] Macdonald, I., *Symmetric functions and Hall polynomials*, 2nd ed., Clarendon Press, Oxford, U.K., 1995.

[MR] Maslen, D. K., and Rockmore, D. N., Separation of variables and the computation of Fourier transforms on finite groups. I, *J. Amer. Math. Soc.* **10** (1997), 169-214.

[Mo] de Montmort, P.R.: Essay d'Analyse sur les Jeux de Hazard, 1st edn. (1708), 2nd edn. (1713). Jacques Quillau, Paris. Reprinted 2005 by AMS/Chelsea, New York.

[NP] Neumann, P. and Praeger, C., Derangements and eigenvalue-free elements in finite classical groups, *J. London Math. Soc.* **58** (1998), 564–586.

[Sc] Schmutz, E., The order of a typical matrix with entries in a finite field, *Israel J. Math* **91** (1995), 349–371.

[Se] Serre, J.-P., On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

[Sh] Shalev, A., A theorem on random matrices and some applications, *J. Algebra* **199** (1998), 124–141.

[St] Stong, R., Some asymptotic results on finite vector spaces, *Adv. Appl Math.* **9** (1988), 167-199.

[VW] Van Lint, J.H. and Wilson, R.M., *A course in combinatorics*. Cambridge University Press, Cambridge, 1992.

Appendix

The purpose of this appendix is to show that the proportion of elements of any coset $gSL(n,q)$ contained in a conjugate of $GL(n/b,q^b).b$ for some prime b is at most $A \cdot \log_2(n)/n^{1/4}$ for a universal constant A. This strengthens Theorem 5.5 (which only considered regular semisimple elements). However the proof technique does not easily extend to the other classical groups.

Let $N(q;d)$ denote the number of monic irreducible degree d polynomials over $\mathbb{F}_q$ with non-zero constant term.

Lemma 6.1.

$$\prod_{d\geq 1}\prod_{i\geq 1}\left(1-\frac{u^d}{q^{id}}\right)^{-N(q;d)} = (1-u)^{-1}.$$

Proof. By switching the order of the infinite products, the lemma follows from the well-known equation (see for instance [F])

$$\prod_{d\geq 1}(1-u^d)^{-N(q;d)} = \frac{1-u}{1-qu}.$$

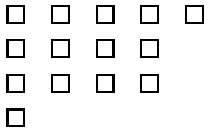
□

Lemma 6.2 will be helpful in upper bounding the proportion of elements of $GL(n,q)$ conjugate to an element of $GL(n/b,q^b)$.

Lemma 6.2. $N(q;db) \leq \frac{1}{b}N(q^b;d)$.

Proof. Recall the Galois theoretic interpretation of roots of an irreducible polynomial as orbits under the Frobenius map. The left hand side is $1/(db)$ multiplied by the number of elements of $\mathbb{F}^*_{q^{db}}$ which form an orbit of size db under the Frobenius map $x \to x^q$. The quantity $N(q^b;d)/b$ is $1/(db)$ multiplied by the number of elements of $\mathbb{F}^*_{q^{db}}$ which form an orbit of size d under the map $x \to x^{q^b}$. The lemma follows. □

For $f(u) = \sum_{n\geq 0} f_n u^n$, $g(u) = \sum_{n\geq 0} g_n u^n$, we let the notation $f << g$ mean that $|f_n| \leq |g_n|$ for all n. In the proof of Theorem 6.3, it will also be useful to have some notation about partitions. Let λ be a partition of some non-negative integer $|\lambda|$ into parts $\lambda_1 \geq \lambda_2 \geq \cdots$. Let $m_i(\lambda)$ be the number of parts of λ of size i, and let λ' be the partition dual to λ in the sense that $\lambda'_i = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$. It is also useful to define the diagram associated to λ by placing λ_i boxes in the ith row. We use the convention that the row index i increases as one goes downward. So the diagram of the partition (5441) is



and λ'_i can be interpreted as the size of the ith column. The notation $(u)_m$ will denote $(1-u)(1-u/q)\cdots(1-u/q^{m-1})$.

Theorem 6.3. *For b prime, the proportion of elements in $GL(n,q)$ conjugate to an element of $GL(n/b, q^b)$ is at most $\frac{A}{n^{1/2}}$ where A is a universal constant.*

Proof. By Lemma 5.4, if an element of $GL(n,q)$ is contained in a conjugate of $GL(n/b,q^b)$, every irreducible factor of its characteristic polynomial either has degree divisible by b or has every Jordan block size occur with multiplicity a multiple of b. By the cycle index of $GL(n,q)$ (see [F] or [St] for background), the proportion of such elements is at the most the coefficient of $u^{n/b}$ in

$$\prod_{d\geq 1}\prod_{i\geq 1}(1-u^d/q^{idb})^{-N(q;db)} \prod_{d\geq 1}\left[\sum_{\lambda\in P_b}\frac{u^{|\lambda|d/b}}{c(q^d,\lambda)}\right]^{N(q;d)}$$

where

$$c(q,\lambda) = \frac{1}{q^{\sum_i(\lambda'_i)^2}\prod_i(1/q)_{m_i(\lambda)}}$$

and P_b is the set of partitions in which each part size occurs with multiplicity a multiple of b.

By Lemma 6.2 and Lemma 6.1,

$$\prod_{d\geq 1}\prod_{i\geq 1}(1-u^d/q^{idb})^{-N(q;db)} << \prod_{d\geq 1}\prod_{i\geq 1}(1-u^d/q^{idb})^{-\frac{1}{b}N(q^b;d)} = (1-u)^{-1/b}.$$

By Lemma 3.2, the coefficient of u^r in this expression is at most $\frac{A}{b\sqrt{r}}$ where A is a universal constant.

Next, we claim that the coefficient of u^s in

$$\prod_{d\geq 1}\left[\sum_{\lambda\in P_b}\frac{u^{|\lambda|d/b}}{c(q^d,\lambda)}\right]^{N(q;d)}$$

is at most q^s divided by the minimum centralizer size of an element of $GL(sb,q)$. To see this, observe that after expanding out the product, the terms correspond to conjugacy classes of $GL(sb,q)$ with the property that every Jordan block corresponding to an irreducible polynomial occurs with multiplicity a multiple of b. These correspond to classes of $GL(s,q)$ and the number of them is at most q^s [MR]. To complete the proof of the claim, recall from [M] that

$$\prod_{\phi} c(q^d,\lambda_\phi)$$

is the centralizer size of an element with conjugacy data $\{\lambda_\phi\}$. Thus Theorem 2.1 implies that the coefficient of u^s in

$$\prod_{d\geq 1}\left[\sum_{\lambda\in P_b}\frac{u^{|\lambda|d/b}}{c(q^d,\lambda)}\right]^{N(q;d)}$$

is at most

$$\frac{A(1+\log_q(bs))}{q^{(b-1)s}}$$

for a universal constant A.

Thus the coefficient of $u^{n/b}$ in

$$\prod_{d\geq 1}\prod_{i\geq 1}(1-u^d/q^{idb})^{-N(q;db)}\prod_{d\geq 1}\left[\sum_{\lambda\in P_b}\frac{u^{|\lambda|d/b}}{c(q^d,\lambda)}\right]^{N(q;d)}$$

is at most

$$\begin{aligned}
&Coef.u^{n/b} in (1-u)^{-1/b} + Coef.u^{n/b} in \prod_{d\geq 1}\left[\sum_{\lambda\in P_b}\frac{u^{|\lambda|d/b}}{c(q^d,\lambda)}\right]^{N(q;d)}\\
&+\sum_{r=1}^{\frac{n}{b}-1} Coef.u^r in (1-u)^{-1/b}\cdot Coef.u^{n/b-r} in \prod_{d\geq 1}\left[\sum_{\lambda\in P_b}\frac{u^{|\lambda|d/b}}{c(q^d,\lambda)}\right]^{N(q;d)}\\
\leq\ & \frac{A}{b\sqrt{n/b}} + \frac{A(1+\log_q(n))}{q^{n-n/b}} + \sum_{r=1}^{n/b-1}\frac{A}{b\sqrt{r}}\frac{(1+\log_q(n-br))}{q^{(b-1)(n/b-r)}}.
\end{aligned}$$

Splitting the sum into two sums (one with $1 \leq r \leq n/(2b)$ and the other with $n/(2b) \leq r \leq n/b - 1$) proves the theorem. □

Now we prove the main results of this appendix.

Theorem 6.4. (1) *For b prime, the proportion of elements of $GL(n,q)$ contained in a conjugate of $GL(n/b, q^b).b$ is at most $\frac{A}{n^{1/2}}$ for a universal constant A.*

(2) *The proportion of elements of $GL(n,q)$ contained in a conjugate of $GL(n/b, q^b).b$ for some prime b is at most $\frac{A \cdot \log_2(n)}{n^{1/2}}$ for a universal constant A.*

Proof. The second part of the theorem follows from the first part together with the fact that an integer n has at most $\log_2(n)$ prime divisors; hence we prove part one.

By Theorem 6.3, the proportion of elements of $GL(n,q)$ conjugate to an element of $GL(n/b, q^b)$ is at most $A/n^{1/2}$ for a universal constant A. Now the number of elements of $GL(n,q)$ conjugate to an element of the group $GL(n/b, q^b).b$ but not to anything in $GL(n/b, q^b)$ is at most the number of conjugacy classes of $GL(n/b, q^b).b$ outside of $GL(n/b, q^b)$ multiplied by the maximum size of a $GL(n,q)$ class. These two quantities are bounded in Theorems 5.2 and 2.1 respectively. One concludes that the proportion of elements of $GL(n,q)$ conjugate to an element of $GL(n/b, q^b).b$ outside of $GL(n/b, q^b)$ is at most

$$\frac{Aq^{n/2}(1 + \log_q(n))}{q^n} \leq A/n^{1/2}.$$

□

Let us consider the same problem for $SL(n,q)$ or more generally for a fixed coset of $SL(n,q)$. Since $[GL(n,q) : SL(n,q)] = q - 1$, the previous result implies that the proportion of elements in a given coset of $SL(n,q)$ conjugate to an element of $GL(n/b, q^b).b$ is at most $(q-1)A/n^{1/2}$ for a universal constant A. So if $q < n^{1/4}$, we see that the proportion of elements of $gSL(n,q)$ in a conjugate of $GL(n/b, q^b).b$ is at most $A/n^{1/4}$.

Suppose that $q \geq n^{1/4}$. Then the proportion of elements in $gSL(n,q)$ which are not regular semisimple is at most $C/q \leq C/n^{1/4}$ for a universal constant C. Arguing as above, we see that every regular semisimple element in $GL(n,q)$ contained in $GL(n/b, q^b)$ has all irreducible factors of its characteristic polynomial of degree a multiple of b. Moreover, we see that the centralizer of such an element (a maximal torus) in $GL(n,q)$ is contained in $GL(n/b, q^b)$. So a maximal torus T_w is conjugate to a subgroup of $GL(n/b, q^b)$ if and only if all cycles of w have length divisible by b. By Lemma 3.3, the proportion of elements in S_n with this property is at most $A/n^{1-1/b}$ for some universal constant A. By [FG1, §5], this implies that the proportion of elements which are regular semisimple and contained in a

conjugate of $GL(n/b, q^b)$ in any fixed coset of $SL(n, q)$ is at most $A/n^{1-1/b}$. Arguing as in the previous theorem shows that the proportion of elements conjugate to an element of $GL(n/b, q^b).b$ outside of $GL(n/b, q^b)$ is at most $A/n^{1/2}$. Summarizing, if $q \geq n^{1/4}$, we have that the proportion of elements of $gSL(n, q)$ which are contained in some conjugate of $GL(n/b, q^b).b$ is at most $D/n^{1/4}$. So we have proved the following:

Theorem 6.5. (1) *For b prime, the proportion of elements of any coset $gSL(n, q)$ contained in a conjugate of $GL(n/b, q^b).b$ is at most $\frac{A}{n^{1/4}}$ for a universal constant A.*

(2) *The proportion of elements of any coset $gSL(n, q)$ contained in a conjugate of $GL(n/b, q^b).b$ for some prime b is at most $\frac{A \cdot \log_2(n)}{n^{1/4}}$ for a universal constant A.*

Almost certainly, the $n^{1/4}$ can be replaced by $n^{1/2}$ and the log factor in (2) can be removed.

Department of Mathematics, University of Southern California, Los Angeles, CA, 90089-2532, USA

E-mail address: fulman@usc.edu

Department of Mathematics, University of Southern California, Los Angeles, CA, 90089-2532, USA

E-mail address: guralnic@usc.edu